



Purdue University  
Center for Education and Research in  
Information Assurance and Security



---

## TCP Session Token Protocol (STOP)

---

Brian Carrier  
Prof. Clay Shields



Center for Education and Research  
in Information Assurance and Security

## Overview

- Based on the Identification Protocol (ident).
- Protocol allows a request to be made for a specific TCP connection based on the IP addresses and port numbers.
- Implemented on OpenBSD, Solaris, and Linux.



## Forensics

- User- and Application-level state data is saved for the process with the requested TCP socket open.
- The server resolves pipes and sockets to identify entire process structure.



## Traceback

- Attackers commonly use a series of hosts before they attack a system to hide their identity, a Connection Chain.
- The protocol traces connection chains by sending traceback requests to the previous host.
- Correlates inbound and outbound TCP sockets by analyzing process structure.



## Logging

- The protocol compensates for the lack of socket and application logging on many UNIX systems.
- Session requests can be sent by a network gateway, to save data for all inbound and outbound connections.



## Privacy

- All responses contain a random token (never the username as ident did).
- User- and application-level data is not revealed until the token is returned to the local administrator.